UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/926,594	11/23/2001	You-Jin Eun	P21705	4083

7055 7590 03/22/2007

GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191

EXAMINER	
DINH, MINH	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	03/22/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/22/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

gbpatent@gbpatent.com
pto@gbpatent.com

Office Action Summary	Application No.	Applicant(s)	
	09/926,594	EUN ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *34-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *34-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 12/19/06.

Response to Arguments

2. Applicant's arguments, see the last paragraph of page 2 and first full paragraph of page 3, filed 12/19/06, with respect to the rejections of claims 34-66 under 35 USC 112, first paragraph, for failing to comply with the written description requirement, i.e., the limitation of claim 34 "storing the system security manager's certificate onto a security kernel of an operating system on a server computer based upon a digital signature of the system security manager" was considered new matter, have been fully considered and are persuasive. The rejections of claims 34-66 under 35 USC 112, first paragraph, for failing to comply with the written description requirement regarding the limitation have been withdrawn.

3. Applicant's arguments, see last paragraph of page 3, with respect to the rejections of claims 34-66 under 35 USC 112, first paragraph, for failing to comply with the written description requirement, i.e., the limitation of claim 34 "setting an access authority of the file system for the user's digital signature keys and certificate" was considered new matter, have been fully

considered but they are not persuasive. None of the passages in the specification referred to by the Applicant discusses setting an access authority of the file system for the user's digital signature keys. According to the specification, the keys themselves are used only for authentication purpose, i.e., for verifying a signature (fig. 10), but not for authorization purpose, i.e., for determining the user's access authority of the file system. Figure 9, steps 908-912, shows that the system does not automatically allow the user to access the file system after successfully authenticating the user's signature, but it must determine the role/access authority the user first and then allows the user to access the file system according to the determined role/access authority.

4. Applicant's arguments, see the last two paragraphs of page 4, with respect to the rejections of claims 34-66 under 35 USC 112, second paragraph, for failing to interrelate elements which are essential to the invention have been fully considered but they are not persuasive. Applicant argues that features of claims 34, 45 and 56 are properly interrelated, and include any features properly characterized as "essential", at least insofar as a person skilled in the art would easily acknowledge the interrelation between the claimed elements (last paragraph). Regarding the independent method claim 34, it recites the steps for generating a system security

manager's digital signature keys and certificate, and storing the system security manager's certificate onto a security kernel of an operating system (lines 4-7); however, neither the keys nor the certificate of the system security manager is recited to be utilized anywhere for the rest of the claim. According to the specification, these elements are essential to the invention, i.e., the secret key of the system security manager is used to sign/generate a user's certificate later and the certificate of the system security manager is used to verify the user's certificate when the user requests to access the file system (fig. 4, element 428; page 12, lines 15-18; fig. 10, steps 1006-1012; page 11, lines 5-19), but, based on the claim language, they can hardly be considered "essential" elements by one of ordinary skilled in the art. Claim 34 also recites the step for generating a user's digital signature keys and certificate (line 8). As discussed above, the specification discloses how the system security manager's digital signature keys and certificate interrelate with the user's digital signature keys and certificate, but claim 34 fails to interrelate those essential elements. Claim 34 further recites the step for identifying a user through a digital signature-based authentication when the user attempts to access the file system (lines 11-12). Because the system security manager acts as a certificate authority (i.e., the system security manager generates the user's certificate) and that the system security manager's certificate is treated as a root certificate, such

authentication would require utilizing not only the user's certificate and but also the system security manager's certificate (fig. 10, steps 1006-1012; page 11, lines 5-19). Again, the claim fails to interrelate those essential elements and, as a whole, such interrelation between the claimed elements would not be easily acknowledged by a person skilled in the art.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 34-66 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 34 also recites the limitation "setting an access authority of the file system for the user's digital signature keys and certificate" (lines 9-10). Whereas the originally filed specification discloses that the user's certificate comprises the access authority of the file system for the user (figure 11, step 1112-1114; figure 4), it does not disclose setting an access authority of the file system for the use's digital signature

keys. Therefore, the limitation is considered new matter. Claims 45 and 56 are rejected on the same basis as claim 34. Claims that are not specifically addressed are rejected by virtue of their dependency.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 34-66 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The invention is directed to a method and system for protecting a file system based on digital signature certificate in which a user's certificate is required to verify the user's signature and access rights, the system security manager's public signature key is required to verify the user's certificate which is generated using the system security manager's private signature key, and the system security manager's certificate is required to retrieve the system security manager's public signature key (figure 10). Specifically, the independent method claim 34 recites the steps for generating a system security manager's digital signature keys and certificate, and storing the system security manager's certificate onto a security kernel of an operating system (lines 4-7); however, neither the keys nor the certificate of the system security manager is recited to be utilized anywhere for the rest of the claim.

According to the specification, these elements are essential to the invention, i.e., the secret key of the system security manager is used to sign/generate a user's certificate later and the certificate of the system security manager is used to verify the user's certificate when the user requests to access the file system (fig. 4, element 428; page 12, lines 15-18; fig. 10, steps 1006-1012; page 11, lines 5-19), but, based on the claim language, they can hardly be considered "essential" elements by one of ordinary skilled in the art. Claim 34 also recites the step for generating a user's digital signature keys and certificate (line 8). As discussed above, the specification discloses how the system security manager's digital signature keys and certificate interrelate with the user's digital signature keys and certificate, but claim 34 fails to interrelate those essential elements. Claim 34 further recites the step for identifying a user through a digital signature-based authentication when the user attempts to access the file system (lines 11-12). Because the system security manager acts as a certificate authority (i.e., the system security manager generates the user's certificate) and that the system security manager's certificate is treated as a root certificate, such authentication would require utilizing not only the user's certificate and but also the system security manager's certificate (fig. 10, steps 1006-1012; page 11, lines 5-19). Again, the claim fails to interrelate those essential elements and, as a whole, such interrelation between the claimed elements

would not be easily acknowledged by a person skilled in the art. Since claim 34 fails to interrelate those elements which are essential to the invention, the claim fails to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 45 and 56 are rejected on the same basis as claim 34. Claims that are not specifically addressed are rejected by virtue of their dependency.

Allowable Subject Matter

9. Subject to the above 112, first and second paragraph rejections, claims 34-66 would be allowable over the prior art of record.

10. The following is a statement of reasons for the indication of allowable subject matter. The present invention is directed to a method for protecting a file system when a user attempts to access the file system wherein a user is first identified through a signature-based authentication using the user's signature certificate and a system security manager's signature certificate, and then the user's access authority of the file system associated with the user's signature certificate is used to determine access authorization. More specifically, independent claims 34, 45 and 56 identify the uniquely distinct feature: storing the system security manager's signature certificate onto a security kernel of an operating system on a server computer. The closest

prior art include: (a) Butt et al. (6,754,829) discloses a similar method for controlling a user request to access a file system by first identifying the user using the user's certificate and a system security manager's signature certificate, which is the root certificate, and then authorizing the request using the user's access authority included in the user's certificate (col. 4, lines 1-51; figures 3, 5-6); however, Butt is silent as to where the system security manager's signature certificate is stored; and (b) Ames et al. ("Security Kernel Design and Implementation: An Introduction") discloses using the security kernel of an operating system to control access to resources (see Implementation considerations, pages 17-20); however, Ames does not disclose using signature certificates. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claims are therefore considered to be in condition for allowance as being novel and nonobvious over prior art

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

3/17/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100